REMARKS

Claims 28-34 are pending in this application. By this Amendment, new claim 34 is added, and claims 28, 30, 32, and 33 are amended. Support for the amendment may be found in at least Fig. 2 (e.g., element 205), Fig. 3 (e.g., step 314), Fig. 4 (e.g., steps 408-418), and paragraphs [0021], [0022], [0024], [0033], [0042], [0044], and [0047] of the Specification in the corresponding published application (U.S. Patent Publication No. 2003/0026432). No new matter is added. Reconsideration of the application is respectfully requested.

Applicant gratefully acknowledges the courtesies extended to Applicant's representatives by Examiner Pyzocha in the January 4 personal interview. Applicant thanks Examiner Pyzocha for his helpful comments. The points discussed during the interview are incorporated into the following remarks.

I. Claims Define Patentable Subject Matter

The Office Action rejects claims 28-33 under 35 U.S.C. § 103(a) as being unpatentable over Wiser et al. (U.S. Patent No. 6,385,596; hereinafter *Wiser*) in view of *Hardjono* (U.S. Patent No. 6,182,214), *Johnston* (U.S. Patent No. 6,373,946), *Arnold* (U.S. Patent No. 6,175,924), *Nakagawa* (U.S. Patent Publication No. 2002/0016775), and further in view of *Chang* (U.S. Patent No. 6,922,735). Applicant respectfully traverses the rejections of claims 28-33.

With respect to independent claim 28, Applicant asserts that the cited prior art fails to disclose or suggest a multiprocessor wireless communication device including at least a security processor to combine a plurality of key-shares, including at least a first key-share, a second key-share, and a device-dependent key-share, and to generate a decryption key to decrypt content for the processing system, the security processor to monitor usage of the content and to purge at least one of the key-shares when the usage exceeds a measurement parameter, as recited in independent claim 28.

First, *Wiser* discloses a secure online music distribution system that provides for secure delivery of audio data and related media over a public communications network (*Wiser*, Abstract). As the Office Action correctly recognizes, *Wiser* does not teach or suggest breaking a decryption key into key shares, one of which is pre-stored on the device (Office Action, pg. 3, ll. 11-12). Therefore, *Wiser* fails to teach, suggest, or render obvious at least a security processor to combine a plurality of key-shares, including at least a first key-share, a second key-share, and a device-dependent key-share, to generate a decryption key to decrypt content for the processing system, as recited in independent claim 28.

Next, the Office Action alleges that *Hardjono* cures the deficiencies of *Wiser* by teaching the use of key shares and pre-storing one on a device (Office Action, page 3, lines 13-14). Applicant respectfully disagrees. *Hardjono* discloses exchanging a secret between a server and one or more multicast clients over an unreliable network (*Hardjono*, Abstract), in which the server divides a secret encryption key K into N shares using a threshold encryption scheme, and transmitting at least one share in each of a plurality of layers of a layered reliable multicast transmission to the multicast clients (*Hardjono*, Fig. 2). Upon receipt of at least M shares, M being less than or equal to N, the clients use the at least M shares to reconstruct the secret (*Hardjono*, col. 3, ll. 37-63).

However, *Hardjono*'s secret exchange server divides encryption key K into N shares independent of the multicast clients (*Hardjono*, Fig. 2; col. 3, ll. 49-52), and the multicast clients combine at least M of N shares to reconstruct the secret without using any key shares that are dependent on the multicast clients' devices. Furthermore, as the Office Action correctly recognizes, *Hardjono*, even in combination with other references, does not teach or suggest purging a key share when usage exceeds a measurement (Office Action, pg. 4, ll. 9-11). Thus, *Hardjono* fails to disclose or render obvious a multiprocessor wireless communication device including at least a security processor to combine a plurality of key-

shares, including at least a first key-share, a second key-share, and a device-dependent key-share, and to generate a decryption key to decrypt content for the processing system, the security processor to monitor usage of the content and to purge at least one of the key-shares when the usage exceeds a measurement parameter, as recited in independent claim 28. Accordingly, a combination of *Wiser* and *Hardjono* would not arrive at the subject matter as recited in claim 28.

The Office Action also alleges that *Nakagawa* cures the deficiencies of *Wiser*, *Hardjono*, and other cited prior art (Office Action, page 4, ll. 13-14). Applicant respectfully disagrees. *Nakagawa* discloses a content control method for restricting a user's operation of a protected content (*Nakagawa*, Abstract) by invalidating or deleting the protected content on the user's contents storage area (*Nakagawa*, Fig. 1; Fig. 6, steps ST5, ST12, ST22, ST32, and ST42; pgs. 4-5, ¶¶ [0071] and [0072]). However, *Nakagawa* does not teach or suggest purging a key-share on a contents control device (*Nakagawa*, Fig. 1, element 100; pg. 2, ¶ [0036]). Thus, *Nakagawa* fails to disclose or render obvious a multiprocessor wireless communication device as recited in independent claim 28. Accordingly, a combination of *Wiser*, *Hardjono*, and *Nakagawa* would not arrive at the subject matter as recited in claim 28.

Johnston discloses using end-to-end encryption and decryption techniques to secure mobile communications between multiple mobile terminals using a common encryption code (*Johnston*, Abstract). The common encryption code in *Johnston* is transmitted to the mobile terminals from a remote database station, and is used to encode and decode data transmitted between the mobile terminals (*Johnston*, Figs. 9-13; col. 9, line 35-col. 11, line 26). *Johnston* discloses a database controller 58 (*Johnston*, Fig. 5) that uses a terminal key K_a to encrypt a cipher key RAND into a second key K_{pa}, and sends it to a mobile terminal (*Johnston*, col. 9, line 57-col. 10, line 31). The mobile terminal then decrypts K_{pa} using terminal key K_a to obtain cipher key RAND (*Johnston*, col. 10, ll. 31-65). Thus, instead of combining key-

shares to generate a decryption key as recited in claim 28, *Johnston* encrypts the cipher key using the terminal key for the mobile terminal to decrypt using an identical terminal key. In addition, *Johnston* fails to mention associating secured content with measurement parameters as recited in claim 28. Therefore, *Johnston* does not teach or suggest a multiprocessor wireless communication device as recited in claim 28.

Arnold teaches certifying the authenticity of an application program before allowing the application program to access a requested data area (*Arnold*, col. 6, ll. 30-41). *Arnold*, however, does not disclose a multiprocessor wireless communication device including at least a security processor that combines a plurality of key-shares, including at least a first key-share, a second key-share, and a device-dependent key-share, and generates a decryption key to decrypt content for the processing system, wherein the security processor monitors usage of the content and purges at least one of the key-shares when the usage exceeds a measurement parameter, as recited in claim 28. *Chang* discloses combining two or more processors on a single integrated circuit, but also fails to teach a multiprocessor wireless communication device as recited in claim 28. Because *Johnston*, *Arnold*, and *Chang* fail to cure the deficiencies of *Wiser* in view of *Hardjono* and further in view of *Nakagawa*, all cited prior art, taken alone or in combination, also would not arrive at the subject matter as recited in claim 28.

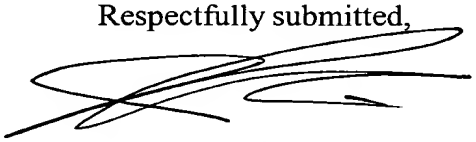
In accordance with the above remarks, Applicant submits that independent claim 28 defines patentable subject matter. Claims 29-34 depend from claim 28, and therefore, also define patentable subject matter, as well as for the additional features they recite. Accordingly, Applicant respectfully requests the withdrawal of the § 103(a) rejections of the claims.

II. Conclusion

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration of claims 28-33 and prompt allowance of claims 28-34 are earnestly solicited.

Should the Examiner believe that anything further would be desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number set forth below.

Respectfully submitted,



James A. Oliff
Registration No. 27,075

Joshua C. Liu
Registration No. 55,391

JAO:JCL

Date: January 31, 2007

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE AUTHORIZATION
Please grant any extension necessary for entry;
Charge any fee due to our Deposit Account No. 15-0461